REMARKS

Applicants respectfully request reconsideration of the above referenced patent application in view of the amendments and remarks set forth herein, and respectfully request that the Examiner withdraw all rejections. Claims 1-3, 7, 8, 11, 22, 29-31, 35 and 26 have been amended. No claims have been canceled. No claims have been added. Thus, claims 1-5, 7-33 and 35-38 are pending.

REJECTIONS UNDER 35 U.S.C. §103

Claims 1-4, 11, 13-16, 18-20, 22, 24-27, 29 and 30-32

These claims are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Davis et al., US Publication No. 2005/0076228 (hereinafter "*Davis*") in view of Ravi et al., US Publication No. 2005/0204155 (hereinafter "*Ravi*") in view of Remer et al., US Patent No. 7,076,653 (hereinafter "*Remer*") in further view of Cromer et al., US Publication No. 2005/0166213 (hereinafter "*Cromer*"). For at least the following reasons, Applicants traverse the above rejection.

Applicants respectfully submit that each of the above rejected claims is not obvious in light of *Davis, Ravi, Remer* and *Cromer*, based at least on the failure of the references to teach or suggest (emphasis added):

> "...each client having a corresponding one of the embedded agents, each embedded agent to store the symmetric cryptographic key in **a secure storage of the client** having the embedded agent, the secure storage accessible to the embedded agent and **not accessible to a host processor on the client having the embedded agent**;
>
> ...wherein the embedded agent of the first client performs an integrity check of a platform of the first client, the integrity check **generating integrity information stored in the secure storage of the first client,...**
>
> wherein **the first client detects a message requesting a secure network connection** for the encrypted traffic flow,
>
> wherein, in response to detecting the message, the embedded agent of the first client verifies, prior to any allowing of the requested secure network connection, that the platform of the first client is not in a compromised state at a time before providing access to the encrypted traffic flow, **the verifying by accessing the integrity information of the secure storage,...**"

as variously recited in current independent claims 1, 11, 22 and 29. The claim amendments are supported in the original disclosure at least by FIGS 2 and 3 and by paragraphs [0028] and [0039] of the specification.

The Office Action alleges that the variously claimed host processor and embedded agent of a client are taught, respectively, by a host processor 130 and a security processor 104 in *Davis*, FIG. 1. In alleging that *Davis* teaches the embedded agent verifying that a platform of the client is not in a compromised state, the Office Action relies upon *Davis*, paragraphs [0038] and [0042], which discuss an authentication input device 136 – e.g. a smart card – for authentication of a user attempting to access host processor 130.

However, the authentication input device 136 is disclosed in *Davis* as being directly attached to host processor 130, where any and all exchanges between authentication input device 136 and security processor 104 are through host processor 130. See, e.g. *Davis* FIG. 1 and paragraph [0038].

Therefore, authentication input device 136 is necessarily accessible to host processor 130. Even assuming *arguendo* that communication between security processor 104 and authentication input device 136 in *Davis* teaches an embedded agent verifying that a client platform is not in a compromised state – which Applicants do not agree – any such communication with security processor 104 is via the host processor 130.

By contrast, current independent claims 1, 11, 22 and 29 variously recite that the claimed verification is performed by accessing integrity information of **a secure storage which is not accessible to the host processor** on the client. For at least the foregoing reasons, *Davis* fails to teach the variously claimed embedded agent of a client verifying, in response to the client detecting a message requesting a secure network connection, that a platform of the client is not in a compromised state, the verifying by accessing integrity information of a secure storage not accessible to a host processor on the client.

Nor do *Ravi*, *Remer* and/or *Cromer* cure the above-described deficiencies of *Davis*. The Office Action relies upon various passages of *Remer* as allegedly supplementing deficiencies of *Davis* regarding verifying a platform state in response to a network connection request. However, *Remer* is simply unrelated to a client verifying a platform state of that same client in response to that same client detecting a network connection request.

Remer is directed to techniques whereby a source entity 50 which is external to a local area network (LAN) 230 seeks connection to a target entity 60 which is within LAN 230. See, e.g. *Remer* FIGS. 3 and 6. Source entity 50 does not send a connection request to target entity 60, but rather to a trusted arbitrator 20b outside of LAN 230. See, e.g. *Remer* col. 3, lines 47-51. Authentications are serially performed between source entity 50 and a trusted arbitrator 20b outside of LAN 230, and then between trusted arbitrator 20b and a connection entity 10b within LAN 230, before any communication is made with target entity 60. See, e.g. *Remer* col. 9, line 50 to col. 10, line 10.

However, nothing in *Remer* teaches whether or how a state of some platform of target entity 60 itself might be verified – by that same target entity 60 – in response to that same target entity 60 detecting a request to connect to source entity 50. Similarly, *Remer* fails to teach an embedded agent of a client verifying, in response to that same client detecting a message requesting a secure network connection, that a platform of that same client is not in a compromised state, the verifying by accessing integrity information of a secure storage not accessible to a host processor on the client.

For at least the foregoing reasons, the cited references fail to either teach or suggest at least one limitation of the invention as variously recited in each of independent claims 1, 11, 22 and 29.

Accordingly, each of independent claims 1, 11, 22 and 29 is non-obvious in light of *Davis, Ravi, Remer* and *Cromer*, as are any claims depending therefrom. For at least the foregoing reasons, Applicants request that the above 35 U.S.C. §103(a) rejection of claims 1-4, 11, 13-16, 18-20, 22, 24-27, 29 and 30-32 based on *Davis, Ravi, Remer* and *Cromer* be withdrawn.

Claims 5 and 33

These claims are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over *Davis, Ravi, Remer* and *Cromer* in further view of Yokota et al., US Publication No. 2002/0164035 (hereinafter "*Yokota*"). For at least the following reasons, Applicants traverse the above rejection.

As demonstrated in the discussion above, there is at least one limitation in each of current independent claim 1, 11, 22 and 29 which is not taught or suggested by *Davis*, *Ravi*, *Remer* and *Cromer*. *Yokota*, which generally relates to the distribution and management of cryptographic keys, does not cure the failure of *Davis*, *Ravi*, *Remer* and *Cromer* to teach or suggest an embedded agent of a client verifying, in response to that same client detecting a message requesting a secure network connection, that a platform of that same client is not in a compromised state, the verifying by accessing integrity information of a secure storage not accessible to a host processor on the client. Therefore, even assuming *arguendo* that all other limitations are obvious in view of *Davis*, *Ravi*, *Remer*, *Cromer* and *Yokota*, which Applicants do not agree, the references nevertheless fail to teach or suggest at least one limitation of the invention as variously recited in each of independent claims 1, 11, 22 and 29.

Accordingly, each of independent claims 1, 11, 22 and 29 – and any claims depending therefrom – is non-obvious in light of *Davis*, *Ravi*, *Remer*, *Cromer* and *Yokota*. Applicants respectfully request that the above 35 U.S.C. §103(a) rejection of claims 5 and 33 based on *Davis*, *Ravi*, *Remer*, *Cromer* and *Yokota* be withdrawn.

Claims 9 and 37

These claims are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over *Davis, Ravi, Remer* and *Cromer* in further view of Walker et al., US Publication No. 2002/0163920 (hereinafter "*Walker*"). For at least the following reasons, Applicants traverse the above rejection.

As demonstrated in the discussion above, there is at least one limitation in each of current independent claims 1 and 29 which is not taught or suggested by *Davis, Ravi,* *Remer* and *Cromer*. *Walker*, which generally relates to techniques for routing packets according to a security association (SA), does not cure the failure of *Davis*, *Ravi*, *Remer* and *Cromer* to teach or suggest an embedded agent of a client verifying, in response to that same client detecting a message requesting a secure network connection, that a platform of that same client is not in a compromised state, the verifying by accessing integrity information of a secure storage not accessible to a host processor on the client. Therefore, even assuming *arguendo* that all other limitations are obvious in view of *Davis*, *Ravi*, *Remer*, *Cromer* and *Walker*, which Applicants do not agree, the references nevertheless fail to teach or suggest at least one limitation of the invention as variously recited in each of independent claims 1, 11, 22 and 29.

Accordingly, each of independent claims 1, 11, 22 and 29 is non-obvious in light of *Davis, Ravi, Remer*, *Cromer* and *Walker*, as are any claims depending therefrom. For at least the foregoing reasons, Applicants request that the above 35 U.S.C. §103(a) rejection of claims 9 and 37 based on *Davis, Ravi, Remer*, *Cromer* and *Walker* be withdrawn.

Claims 10, 17, 28 and 38

These claims are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over *Davis*, *Ravi*, *Remer*, *Cromer* and in further view of Ylonen, USPN 6,782,474 (hereinafter "*Ylonen*"). For at least the following reasons, Applicants traverse the above rejection.

As demonstrated in the discussion above, there is at least one limitation in each of current independent claim 1, 11, 22 and 29 which is not taught or suggested by *Davis*, *Ravi*, *Remer* and *Cromer*. *Ylonen*, which generally relates to network configuration using device-specific configuration packets, does not cure the failure of *Davis*, *Ravi*, *Remer* and *Cromer* to teach or suggest an embedded agent of a client verifying, in response to that same client detecting a message requesting a secure network connection, that a platform of that same client is not in a compromised state, the verifying by accessing integrity information of a secure storage not accessible to a host processor on the client. Therefore, even assuming *arguendo* that all other limitations are obvious in view of

Davis, *Ravi*, *Remer*, *Cromer* and *Ylonen*, which Applicants do not agree, the references nevertheless fail to teach or suggest at least one limitation of the invention as variously recited in each of independent claims 1, 11, 22 and 29.

Accordingly, each of independent claims 1, 11, 22 and 29 is non-obvious in light of *Davis*, *Ravi*, *Remer*, *Cromer* and *Ylonen*, as are any claims depending therefrom. For at least the foregoing reasons, Applicants request that the above 35 U.S.C. §103(a) rejection of claims 10, 17, 28 and 38 based on *Davis*, *Ravi*, *Remer*, *Cromer* and *Ylonen* be withdrawn.

Claims 12 and 23

These claims are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over *Davis, Ravi, Remer* and *Cromer* in further view of Grohoski et al., US Publication No. 2004/0225885 (hereinafter "*Grohoski*"). For at least the following reasons, Applicants traverse the above rejection.

As demonstrated in the discussion above, there is at least one limitation in each of current independent claims 11 and 22 which is not taught or suggested by *Davis, Ravi, Remer* and *Cromer*. *Grohoski*, which generally relates to use of a cryptographic co-processor, does not cure the failure of *Davis*, *Ravi*, *Remer* and *Cromer* to teach or suggest an embedded agent of a client verifying, in response to that same client detecting a message requesting a secure network connection, that a platform of that same client is not in a compromised state, the verifying by accessing integrity information of a secure storage not accessible to a host processor on the client. Therefore, even assuming *arguendo* that all other limitations are obvious in view of *Davis*, *Ravi*, *Remer*, *Cromer* and *Grohoski*, which Applicants do not agree, the references nevertheless fail to teach or suggest at least one limitation of the invention as variously recited in each of independent claims 1, 11, 22 and 29.

Accordingly, each of independent claims 1, 11, 22 and 29 is non-obvious in light of *Davis, Ravi, Remer*, *Cromer* and *Grohoski*, as are any claims depending therefrom. For at least the foregoing reasons, Applicants request that the above 35 U.S.C. §103(a) rejection of claims 12 and 23 based on *Davis, Ravi, Remer*, *Cromer* and *Grohoski* be withdrawn.

Claim 21

This claim is rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over *Davis, Ravi, Remer* and *Cromer* in further view of Kramer et al., US Publication No. 2005/0201554 (hereinafter "*Kramer*"). For at least the following reasons, Applicants traverse the above rejection.

As demonstrated in the discussion above, there is at least one limitation in current independent claim 11 which is not taught or suggested by *Davis, Ravi, Remer* and *Cromer*. *Kramer*, which generally relates to encryption techniques using a cipher counter, does not cure the failure of *Davis*, *Ravi*, *Remer* and *Cromer* to teach or suggest an embedded agent of a client verifying, in response to that same client detecting a message requesting a secure network connection, that a platform of that same client is not in a compromised state, the verifying by accessing integrity information of a secure storage not accessible to a host processor on the client. Therefore, even assuming *arguendo* that all other limitations are obvious in view of *Davis*, *Ravi*, *Remer*, *Cromer* and *Kramer*, which Applicants do not agree, the references nevertheless fail to teach or suggest at least one limitation of the invention as variously recited in each of independent claims 1, 11, 22 and 29.

Accordingly, ach of independent claims 1, 11, 22 and 29 is non-obvious in light of *Davis, Ravi, Remer*, *Cromer* and *Kramer*, as are any claims depending therefrom. For at least the foregoing reasons, Applicants request that the above 35 U.S.C. §103(a) rejection of claim 21 based on *Davis, Ravi, Remer*, *Cromer* and *Kramer* be withdrawn.

CONCLUSION

For at least the foregoing reasons, Applicants submit that all pending objections and/or rejections have been overcome. Therefore, all pending claims are in condition for allowance and such action is earnestly solicited. The Examiner is respectfully requested to contact the undersigned by telephone if such contact would further the examination of the present application. Please charge any shortages and credit any overcharges to our Deposit Account number 02-2666.

Respectfully submitted,
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN, LLP

Date: April 15, 2010

/Dermot G. Miller/
Dermot G. Miller
Attorney for Applicants
Reg. No. 58,309

1279 Oakmead Parkway
Sunnyvale, CA 94085-4040
(503) 439-8778